UNITED STATES DISTRICT COURT

DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA v. TIMOTHY LIVINGSTON, Defendant.	Hon. William J. Martini Crim. No. 15-CR-626 (WJM)

In Limine Motions of Defendant, Timothy Livingston

LORRAINE S. GAULI-RUFO
130 Pompton Avenue
Verona, NJ 07044

KARL S. KRONENBERGER
ANSEL J. HALLIBURTON
KRONENBERGER ROSENFELD, LLP
150 Post St., Suite 520
San Francisco, CA 94105

Attorneys for Defendant Timothy Livingston

PRELIMINARY STATEMENT

Defendant Timothy Livingston ("Mr. Livingston" or the "Defendant"), through his undersigned attorney, files these Motions *In Limine,* seeking an Order for the following relief:

a) excluding any reference to "phishing" and/or the sign or picture "<><";

b) prohibiting reference to or introduction of any images or reference to Mr. Livingston's Ferrari or Cadillac Escalade vehicles at trial, and excluding Government Exhibits 2003, 2004 and 8001;

c) excluding Government Exhibit 4001 (FTC Search Data);

d) excluding Government Exhibit 2030 (image of a man with Down's Syndrome found on Mr. Livingston's computer);

e) excluding Government Exhibit 6001 (notification of a Gmail user to Brass Ring);

f) excluding Government Exhibit 7011 (an email thread produced by Digital Treetop);

g) objecting to the chain of possession and authenticity of the evidence the government seeks to admit;[1] and

h) to preclude the government's expert, John R. Levine, from testifying on topics on which he is unqualified, and from explaining the law.

[1] *See* Certification of Lorraine Gauli-Rufo, attached hereto.

In support, Mr. Livingston provides the following legal and factual arguments.

I. BACKGROUND

A six-count Superseding Indictment was filed on July 8, 2016, charging Timothy Livingston with conspiracy to commit fraud and related activity in connection with computers and access devices (18 U.S.C. 371); conspiracy to commit fraud and related activity in connection with electronic mail (18 U.S.C. 1037(a)–(b) (the CAN-SPAM Act)); accessing a computer in furtherance of fraud (18 U.S.C. 1030(a)(4) & (c)(3)(A) (parallel Computer Fraud and Abuse statute); intentionally damaging a computer by knowing transmission of a program, information, code or command (18 U.S.C. 1030(a)(5)(A) & (c)(4)(B)); using or trafficking in an unauthorized access device (18 U.S.C. 1029(a)(2) & (c)(1)(a)(i)); and aggravated identify theft (18 U.S.C. 1028A(a)(1) & (2)). Counts 2 and 3 center on co-defendant Tomasz Chmielarz's authorship of, and Mr. Livingston's use of, a program that visited Corporate Victim #2's website and (allegedly without authorization) used a form on it to send email. Counts 5 and 6 involve alleged use of "usernames and passwords" from Corporate Victim #1.

The Defendant filed pre-trial motions on September 16, seeking, *inter alia*, to dismiss Counts 2, 3, 5, and 6 of the Indictment. The gist of the Defendant's position is that the Government knew, or should have known, that virtually all the internet conduct it alleges as unlawful is standard (and lawful) procedure in the commercial emailing industry.[2]

[2] *E.g.*, mass email data obtained by legitimate bulk email account creation, legitimate use of leased servers, failure to disclose that software with potential to access others' account had not been used for months prior to website creation and also could be used for lawful generation of accounts, lawful use of

The Government filed on August 23, 2016 a motion to introduce under FRE 404(b) several chat messages significantly predating the conspiracy alleged in this case (August 2012 to September 2015), which it contends are highly probative of motive, intent, preparation, plan, knowledge, and absence of mistake notice.[3] On October 7, 2016, the Government also sought leave to introduce Exhibit 1131, a November 8, 2010 chat between *rpliving912* and *craigslistpostingpro* (assertedly highly probative of the same factors). Following a hearing on the Pretrial motions on October 13, 2016, Your Honor reserved decision on Mr. Livingston's Motions to Dismiss and the Government's 404(b) motion.

II. ARGUMENT

A. None of the chats that are outside the timeline of the alleged conspiracy should be permitted to be introduced as Government Exhibits, nor should any reference to "phishing" and or the sign or symbol "<><."[4]

a. The chats and references to phishing and or the symbol "<><" are not probative of motive, opportunity, intent, preparation, plan, knowledge or identity.

multiple domain names, consumer complaints based on faulty understanding of law, failure to acknowledge that overwhelming amount of credentials on website were for Defendant-generated accounts, suggestion that Verizon statements alleged breach of its own servers, when it did not.

[3] September 27, 2010 chat between *rpliving912* and *red7aff* to establish code symbol for phish; January 20, 2011 chat between *rpliving912* and *amalgamltd* to establish phish means hacked accts; April 25, 2010 chat between *rpliving912* and *contact20033* to establish use of hacked accts for spam purposes; October 14, 2010 Chat between *rpliving912* and *jwhitebiz* to show profit motive.

[4] While the Government brought a motion *in limine* to admit the chats subject to this motion and the defense responded to it, the defense brings its own *in limine* to preclude the introduction of these chats that are outside the time of the conspiracy and seek by its introduction to prove an element of some of the charged offenses.

Federal Rule of Evidence 404(b) provides in pertinent part:

> Evidence of other crimes, wrongs, or acts is not admissible to prove the character of a person in order to show action in conformity therewith. It may, however, be admissible for other purposes, such as proof of motive, opportunity, intent, preparation, plan, knowledge, identity, or absence of mistake or accident.

Because prior acts evidence "has a unique potential to distract the jury, inflame emotions, or arouse prejudices by reflecting negatively on a defendant's character," the Third Circuit requires that such evidence be admitted on narrow grounds and only after careful analysis. *United States v. Washington,* No. 13-1847 (3rd Cir. 2015) (non-precedential), citing *United States v. Caldwell*, 760 F.3d at 277. To satisfy the requirements of Rule 404(b), relevant evidence of other acts must have a proper evidentiary purpose and not be substantially more prejudicial than probative. *United States v. Cross*, 308 F.3d 308. 320–21 (3d Cir. 2002) (footnote omitted). Rule 404(b) evidence must be for a purpose other than to demonstrate a defendant's bad character in order to encourage the jury to convict on the basis of a propensity to commit crime. *United States v. Green*, 617 F.3d 233, 248–48 (3d Cir. 2010). Evidence of prior bad acts is excluded unless "the proponent can demonstrate that the evidence is admissible exclusively for a non-propensity purpose." *United States v. Caldwell*, 760 F.3d 267 (3rd Cir. 2014). No link of the chain of inferences can connect to forbidden propensity. *Ibid.* See also *United States v. Davis*, 726 F.3d 434, 441 (3d Cir. 2013) (citing *United States v. Green*, 617 F.3d at 239).

The line between plan/modus operandi and propensity is often thin and involves pinpointing the "essential fact" sought to be proved by the evidence. *Becker v. Arco Chemical Co.*, 207 F.3d 176, 195 (3rd Cir. 2000). The Government contends here that

the prior chats establish coded language for phishing and the defendant's knowledge that phishing was unauthorized entry into other individuals' email accounts. From these chats, the Government seeks to infer intentional unlawful acts in the charged offense, not plan/modus operandi as it contends. Indeed, without these pre-conspiracy chats, the Government has no intentional unlawful act evidence because — as the defense shows in its argument to dismiss — the practices the Government alleges as unlawful are entirely consistent with legitimate, commercial bulk email industry practices. In order for the pre-conspiracy chats to be admitted as 404(b) modus operandi evidence, they must show similar acts as that alleged in the charged crime. *Becker*, at 200. These don't. Introduction of these pieces of evidence is sought to show exactly what is *missing* in the charged offense: intentional use of another's account to promote spam. It is therefore inadmissible under 404(b). See *Becker*, at 203, citing *J&R Ice Cream v. California Smoothie*, 31 F.3d 1259, 1269 (3d Cir. 1994) (evidence to show prior intent to discriminate tantamount to propensity evidence and therefore not admissible under 404(b)).

Indeed, it can be questioned whether these pre-conspiracy chats are extrinsic evidence at all. Conduct that is an element of the charged offense (intrinsic evidence) is not admissible under Rule 404(b). *United States v. Green*, *supra*. And, courts admit intrinsic evidence of events or conduct occurring before the conspiratorial period charged in the indictment only where the conspiracy is alleged to be a continuing one. See *United States v. United States Gypsum Co.*, 600 F.2d 414, 417–18 (3d Cir.), cert. denied, 444 U.S. 884 (1979). Such is not the case here. The Government cannot

"backdoor" in pre-conspiracy evidence under 404(b) when it hasn't a case without it.[5]

b. The chats' prejudicial impact outweighs their probative value.

Evidence sought to be admitted under Rule 404(b) may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence. See *United States v. Bergrin*, 682 F.3d 261 (3rd Cir. 2012) Here, the prejudicial impact of the chats is significant in that they present direct discussion of phishing and hacking concepts, conduct which is wholly lacking during the conspiracy period. The discussions are distinct in nature from the conduct alleged in the indictment, which is based on basic, commercial bulk emailing practices. Because of this distinction, inclusion of the chats will blur the issue for the potential jurors and conflate the two, encouraging the erroneous conclusion that any bulk email program constitutes unlawful hacking or phishing. The chats also significantly precede the timeline of the alleged conspiracy, again increasing their prejudicial impact, and weakening their probative value. There is a substantial risk that introduction of the chats will unfairly prejudice the jury against the Defendant, and for that reason as well, they should be excluded.

[5] None of the chats sought to be introduced by the Government involve any individual (other than the Defendant) either named as a co-conspirator or capable of being an unidentified co-conspirator during the scope of the alleged conspiracy. There is no identity of interest between the speaker of these statements and the Defendant. Accordingly, no hearsay exception applies. *United States v. Weaver*, 507 F.3d 178, 181 (3d Cir. 2007).

B. Any reference to luxury vehicles, specifically a Ferrari and a Cadillac Escalade owned by Mr. Livingston, including Government Exhibits 2003, 2004, 5102, 5301, and 8001, should be excluded from being introduced at trial because the prejudice of introducing this evidence substantially outweighs any probative value.

Mr. Livingston seeks an order barring any reference to a Ferrari or a Cadillac Escalade owned by him. The fact of owning luxury vehicles has absolutely no bearing on any fact at issue in this case, and would only serve the inflammatory, and irrational, inference that any personal wealth of the Defendant must necessarily be due to unlawful activities. FED. R. EVID. 401, 402, 403. This motion also pertains to Government Exhibit 8001, which is a summary chart that includes references to these vehicles.

C. Government Exhibit 4001 (FTC Search Data) should be excluded from admission at trial pursuant to the Confrontation Clause of the Sixth Amendment, as well as Rules 401, 403, 802, 803, and 1002 of the Federal Rules of Evidence, among others.

This motion *in limine* is about the Government's Trial Exhibit 4001, which the Government's exhibit list describes as "FTC Search Data". Mr. Livingston brings this motion under the Confrontation Clause of the Sixth Amendment, as well as Rules 401, 403, 802, 803, and 1002 of the Federal Rules of Evidence, among others.

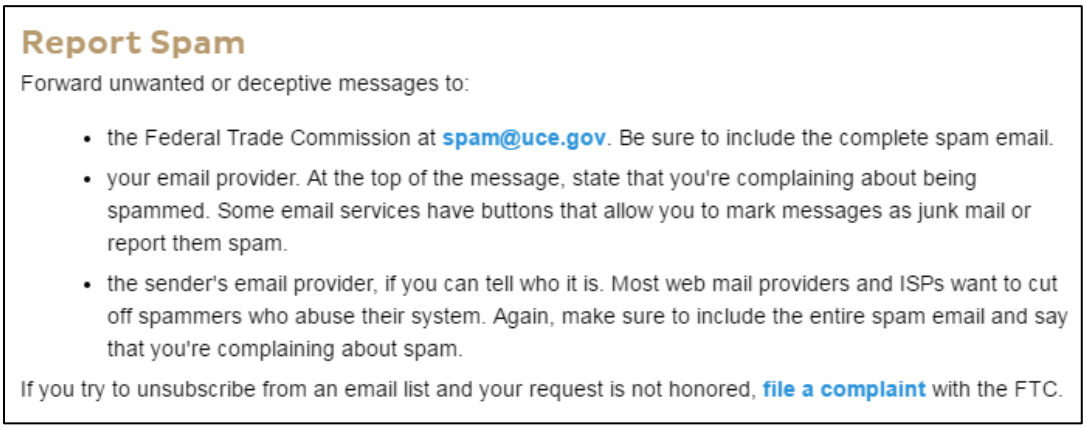
Exhibit 4001 consists of thousands of emails purportedly collected by the Federal Trade Commission. Mr. Livingston believes the Government will try to use Exhibit 4001 as evidence that Mr. Livingston sent specific emails to consumers, and that those emails are evidence of the conspiracies and other offenses with which the Government has charged him.

Among its many problems, Exhibit 4001 contains multiple levels of hearsay

statements by unknown and anonymous declarants, statements by computer programs of unknowable reliability, and numerous clearly irrelevant items with no connection to Mr. Livingston nor to any offense charged in the Superseding Indictment. While any one of these problems is sufficient for the Court to exclude, taken together, it would be an abuse of discretion and a violation of Mr. Livingston's constitutional rights for the Court to allow Exhibit 4001 into evidence. The Court should exclude Exhibit 4001 in its entirety, and should preclude the Government from making any reference to the FTC's unreliable spam database at trial.

a. Background on the FTC Spam Database

On its website, the FTC asks the general public to forward it copies of "unwanted or deceptive" email:



Report Spam

Forward unwanted or deceptive messages to:

- the Federal Trade Commission at **spam@uce.gov**. Be sure to include the complete spam email.
- your email provider. At the top of the message, state that you're complaining about being spammed. Some email services have buttons that allow you to mark messages as junk mail or report them spam.
- the sender's email provider, if you can tell who it is. Most web mail providers and ISPs want to cut off spammers who abuse their system. Again, make sure to include the entire spam email and say that you're complaining about spam.

If you try to unsubscribe from an email list and your request is not honored, **file a complaint** with the FTC.

Federal Trade Commission, *Spam*, https://www.consumer.ftc.gov/articles/0038-spam [https://perma.cc/5WPQ-NM9F].

Once an email is forwarded to the FTC, it is put into a database. Very little information is publicly available about the operation of the FTC's spam database. However, a 2004 press release touts the FTC's ability to collect spam email, as well as

the use of the collected information by both the FTC and "law enforcement partners". The press release says the FTC's spam collection is for the express purpose of "generat[ing] cases":

> The FTC and its **law enforcement partners use the database to generate cases** against people who use spam to spread false or misleading information about their products or services.

Federal Trade Commission, "FTC Unveils New E-mail Address for Deceptive Spam: Spam@uce.gov" (Jul. 28, 2004), https://www.ftc.gov/news-events/press-releases/2004/07/ftc-unveils-new-e-mail-address-deceptive-spam-spamucegov [https://perma.cc/E74Z-5UZ6] (emphasis added).

An FTC Privacy Impact Assessment contains further details on the operation of its spam database, and discloses that the FTC shares the database with "thousands of civil and criminal law enforcement personnel in the United States and abroad through a secure Internet website called the Consumer Sentinel Network." Federal Trade Commission, *Privacy Impact Assessment for Sentinel Network Services* (Jan. 2016) at p. 2, https://www.ftc.gov/system/files/attachments/privacy-impact-assessments/160114snspia.pdf [https://perma.cc/QE75-YVZP]. The Privacy Impact Assessment also states that "the Commission's website notifies consumers that the FTC maintains this information for use in law enforcement investigations." *Id.* at 5.

b. Confrontation Clause Violation

As discussed below, spam complaints to the government are testimonial statements, and their introduction in a criminal trial presents serious issues under the

Confrontation Clause.

The Sixth Amendment to the United States Constitution guarantees that, "In all criminal prosecutions, the accused shall enjoy the right…to be confronted with the witnesses against him…" U.S. Const. amend. VI. The Supreme Court has explained that the "central concern of the Confrontation Clause is to ensure the reliability of the evidence against a criminal defendant by subjecting it to rigorous testing in the context of an adversary proceeding before the trier of fact." *Maryland v. Craig*, 497 U.S. 836, 845 (1990). The Confrontation Clause can *only* be satisfied by the opportunity to cross-examine the declarant:

> Where testimonial evidence is at issue…the Sixth Amendment demands what the common law required: unavailability and a prior opportunity for cross-examination… Where testimonial statements are at issue, the only indicium of reliability sufficient to satisfy constitutional demands is the one the Constitution actually prescribes: confrontation.

Crawford v. Washington, 541 U.S. 36, 68–69 (2004). Statements are testimonial if they are "taken for use at trial":

> Whether formal or informal, out-of-court statements can evade the basic objective of the Confrontation Clause, which is to prevent the accused from being deprived of the opportunity to cross-examine the declarant about statements taken for use at trial.

Michigan v. Bryant, 562 U.S. 344, 358 (2011).

While certain narrow exceptions to this rule exist — such as 911 calls (*Davis v.*

Washington, 547 U.S. 813 (2006)), dying declarations (*Michigan v. Bryant*, 562 U.S. 344 (2011)), and face-to-face confrontation of child abuse victims by their alleged rapists (*Craig* at 852–53) — this case presents no such compelling interest or exception. This is a case about email. The government *could* compel the attendance of those who allegedly received email spam and forwarded it to the FTC, and those people *could* testify. But if the government *chooses* not to bring those alleged email recipients to Mr. Livingston's criminal trial, then the Court must recognize that choice for what it is: a violation of Mr. Livingston's constitutional rights under the Confrontation Clause of the Sixth Amendment.

The FTC's spam database is the online equivalent of an anonymous tip line. While anonymous tips may *sometimes* contribute to probable cause for a search in the Fourth Amendment context, *Illinois v. Gates*, 462 U.S. 213 (1983), they may *never* form the exclusive support for a search, *Florida v. J. L.*, 529 U.S. 266 (2000), and the plain meaning of the Confrontation Clause makes clear that they are *never* admissible *at trial* as evidence of an offense. U.S. Const. amend. VI; *Crawford v. Washington*, 541 U.S. 36, 68–69. While many cases discuss whether anonymous tips are enough to justify an investigatory stop or a search, *see generally United States v. Ritter*, 416 F.3d 256, 261–265 (3d Cir. 2005) ("close case" regarding search warrant based in part on anonymous tips), it is perhaps because the proposition is so obviously unconstitutional that it is much harder to find cases on the use of anonymous tips *as substantive evidence at trial*. Those few cases tend to involve decisions by defendants to not contest the admission of anonymous tips. *See, e.g.*, *United States v. Simpson*, 182 Fed. App'x 84, 86 (3d Cir.

2006) (no error in admitting anonymous tip because defendant failed to object to, and relied on, tip at trial). The opposite is true here, where Mr. Livingston vigorously contests any admission of evidence from the FTC's spam database.

The recent case of *Woods v. Etherton*, 136 S. Ct. 1149 (2016) (per curiam), is distinguishable both procedurally and on its facts. In that case, the prosecution repeated several times at trial that an anonymous tip led police to arrest the defendant, after which cocaine was found in his possession. However, a key eyewitness had testified and corroborated the content of the tip. Procedurally, the case is quite different from this one: in *Etherton*, the Supreme Court held that the Sixth Circuit had applied the wrong legal standard, and reversed the Circuit court's finding of ineffective assistance of counsel for the defendant's lawyer's failure to raise a Confrontation Clause violation. This case, however, presents the very different *substantive* issue of whether anonymous tips are admissible under the Confrontation Clause — not whether counsel was ineffective for failing to raise that issue. In this case, there are no other admissible sources for the information in Exhibit 4001. This is unlike *Etherton*, where there was other eyewitness testimony that could render the admission of the anonymous tip harmless error. Borrowing from *Etherton*'s facts, Exhibit 4001 is not just the anonymous tip, but also the cocaine itself — and without the eyewitness testimony. The Supreme Court's reasoning in *Etherton* does not stretch to these facts, to which the Confrontation Clause's plain meaning should be applied.

i. Defendant is Unable to Challenge the Credibility of the Declarants Because Their Identities Are Unknown.

Rule 806 of the Federal Rules of Evidence fleshes out and implements the purpose of the Confrontation Clause, requiring that a defendant have an opportunity to challenge the credibility of a hearsay declarant's statements. FED. R. EVID. 806.

Even if the Government wanted to present testimony by persons in the FTC database, that is *practically* impossible because of the nature of the database and what it contains. Here, many of the emails in Exhibit 4001 contain insufficient information to know who their authors are. How, then, can Mr. Livingston exercise his rights under Rule 806 and the Confrontation Clause? The answer is that he cannot, and therefore the evidence cannot be admitted.

ii. Some of the Declarants are Computer Programs, Not Humans, and Cannot be Cross-Examined or Even Evaluated for Accuracy.

Several emails in Exhibit 4001 include this text: "Once removed with that method, this Complaint Generator tool will create no more requests on this domain." (Edman Decl. ¶ 28; Declaration of Ansel Halliburton in Support of Defendant's Motions *in Limine* ("Halliburton Decl.") Ex. 10) (example of email within Government's Trial Exhibit 4001). This appears to indicate that several of the email complaints included in the FTC's spam database, and subsequently in Exhibit 4001, are not actually submissions by humans — but are, instead, the output of unknown automated "Complaint Generator tool" computer programs. (Edman Decl. ¶ 29.)

In *Bullcoming v. New Mexico*, 564 U.S. 647 (2011), the Supreme Court held that

the Confrontation Clause was violated when a government laboratory analyst testified about another non-testifying analyst's work. Here, the government is advancing analysis performed — and submitted — by fully automated software. Mr. Livingston cannot put this software on the stand and cross-examine it. Nor is anything else about this software evident from the contents of Exhibit 4001. And while the Government will presumably attempt to substitute the testimony of its technical expert, *Bullcoming* teaches that this is not an acceptable substitute at all. *See also* FED. R. EVID. 602, 901.

Another potential analogy is to red-light cameras. First, of course, such cameras are used primarily to give speeding tickets — not to put the accused in federal prison. But even when they are used, courts require proof that they are reliable. *See*, *e.g.*, *Business owner casts reasonable doubt on accuracy of speed cameras*, THE WASHINGTON TIMES, http://www.washingtontimes.com/news/2011/apr/20/business-owner-casts-reasonable-doubt-on-accuracy-/ [https://perma.cc/E9YZ-KTZZ]. There is not even a hint that the Government intends to present such evidence in this case. The Court must exclude these automated statements.

If Mr. Livingston cannot question his accusers about their statements — and the Government clearly intends to use the contents of Exhibit 4001 to prove its accusations against him — then those statements are inadmissible under the Confrontation Clause.

c. Exhibit 4001 Consists Entirely of Testimonial Hearsay.

In this criminal case about email spam, the Government will have to present evidence of the actual emails it contends Mr. Livingston sent in violation of the CAN-SPAM Act and other federal statutes. From the Government's exhibit list, it appears this

evidence will come primarily from Exhibit 4001.

In *Crawford v. Washington*, 541 U.S. 36 (2004), a landmark Confrontation Clause case, the Supreme Court held that testimonial hearsay statements from unavailable witnesses were inadmissible because they violated the Confrontation Clause.

Here, the Government wishes to introduce emails from unknown persons — without the testimony of those unknown persons.

i. The Government Will Use the Emails in Exhibit 4001 to Prove the Truth of the Matters Asserted in Them.

The emails in Exhibit 4001 are testimonial hearsay. They are — purportedly — copies of emails that unknown persons received, and then forwarded to the FTC, and which the FTC then saved into its database. The Government will present these emails in support of its case-in-chief against Mr. Livingston. The Government will present these emails to prove their contents, including what the emails purportedly said, when their unknown recipients purportedly received them, the purported contents of the email headers (although the unknown recipients preserved only some of them). The Government will then attempt to tie Mr. Livingston to these emails, and to convict him of crimes with them.

It is clear that the Government wishes to use Exhibit 4001 for the truth of the matters they assert, *i.e.*, the transmission of certain allegedly violative emails by Mr. Livingston to certain unknown recipients.

In *United States v. Silva*, 380 F.3d 1018, 1020 (7th Cir. 2004), the Seventh Circuit reversed the conviction of a drug defendant for extensive violations of the

hearsay rule and the Confrontation Clause. At trial, the court had allowed a DEA agent's testimony about a non-testifying confidential informant's conversations with another non-testifying person, as well as a police officer's testimony about the results of a lab analysis that he did not perform. Writing for the appellate court, Judge Easterbrook found the trial judge's reasoning that the hearsay testimony was "not being offered for the truth of the matter" perplexing, writing "That's surprising, for the evidence directly inculpated Silva. See Fed.R.Evid. 801(c)." *United States v. Silva*, 380 F.3d 1018, 1019 (7th Cir. 2004). The court further explained that "[a]llowing agents to narrate the course of their investigations, and thus spread before juries damning information that is not subject to cross-examination, would go far toward abrogating the defendant's rights under the sixth amendment and the hearsay rule." *United States v. Silva*, 380 F.3d 1018, 1020 (7th Cir. 2004).

Here, where the FTC has touted its spam database as a way to collect evidence and "build[] cases" with its "law enforcement partners", who include "thousands of civil and criminal law enforcement personnel in the United States and abroad", everything in Exhibit 4001 should be treated as testimonial. Again, analogizing the FTC database to anonymous tips or confidential informants is helpful: "When a confidential informant gives information to a police officer for use in a criminal investigation, the statements are testimonial regardless of the 'formality' of the statements." 2 Wharton's Criminal Evidence § 6:10.20 (15th ed.) (2015), *citing United States v. Cromer*, 389 F.3d 662, 675, (6th Cir. 2004) ("Tips provided by confidential informants are knowingly and purposely made to authorities, accuse someone of a crime, and often are used against the accused

at trial. The very fact that the informant is confidential — *i.e.*, that not even his identity is disclosed to the defendant — heightens the dangers involved in allowing a declarant to bear testimony without confrontation. The allowance of anonymous accusations of crime without any opportunity for cross-examination would make a mockery of the Confrontation Clause.").

ii. The Government's Witnesses Cannot Cure Exhibit 4001's Constitutional and Evidentiary Deficiencies.

Someone must testify to authenticate the *substantive contents* of Exhibit 4001. FED. R. EVID. 901. While the Government has disclosed to the defense *one* instance of identifying and speaking with an alleged recipient of *one* of these thousands of emails, there is nobody with any personal knowledge to testify to receiving the remaining vast majority of the emails in Exhibit 4001, or to their accurate representation in Exhibit 4001.

While the Government's technical expert might be permitted to opine on how the jury should interpret Exhibit 4001, he is not a fact witness, and he can authenticate nothing. Nor even could any FTC employee or contractor, because FTC employees and contractors did not send *the underlying emails* comprising Exhibit 4001. At most, an FTC employee or contractor might testify about what the FTC's technology systems do once they receive emails from unknown senders. But neither any FTC employee or contractor nor the Government's technical expert have personal knowledge from which the testimonial evidence in Exhibit 4001 must be authenticated as being "what [the Government] claims it is". FED. R. EVID. 901.

It would be a further Confrontation Clause violation if the Court were to rely on the Government's witnesses' anticipated testimony that the FTC's database, and the emails within it, are reliable: "Dispensing with confrontation because testimony is obviously reliable is akin to dispensing with jury trial because a defendant is obviously guilty. This is not what the Sixth Amendment prescribes." *Crawford v. Washington*, 541 U.S. 36, 62 (2004).

d. Exhibit 4001 Does Not Contain Public Records or Business Records Within the Meaning of the Federal Rules of Evidence.

Exhibit 4001 does not contain "public records" within the meaning of Rules 803 or 901, and thus can neither escape the hearsay rule nor be authenticated as such.

i. The Emails Received by the FTC Are Not Admissible as Public Records.

Rule 803(8) provides the public records exception to the hearsay rule. The Rule states that evidence from a "record or statement of a public office" qualifies for this exception if:

> (A) it sets out:
>
> > (i) the office's activities;
> >
> > (ii) a matter observed while under a legal duty to report, but not including, in a criminal case, a matter observed by law-enforcement personnel; or
> >
> > (iii) in a civil case or against the government in a criminal case, factual findings from a legally authorized investigation; and

(B) the opponent does not show that the source of information or other circumstances indicate a lack of trustworthiness.

FED. R. EVID. 803(8). Both subsections (A) and (B) must be satisfied; neither are.

First, (A)(i) does not apply because Exhibit 4001 does not contain records of the Federal Trade Commission. Instead, it contains emails that unknown persons on the Internet purportedly received and forwarded to the FTC. Therefore it does not "set[] out…the office's activities". FED. R. EVID. 803(8)(A)(i). Second, (A)(ii) does not apply because neither the FTC nor any of its staff "observed" anything, nor is the FTC a "law-enforcement" agency; it has no power to bring criminal cases. FED. R. EVID. 803(8)(A)(ii); 41 U.S.C. § 46(k) (FTC may only refer information to other agencies for criminal prosecution). Third, (A)(iii) does not apply because this is a criminal case, and it is the Government advancing Exhibit 4001, not the defendant. Subsection (B) also fails, because Mr. Livingston has made a substantial showing that the "trustworthiness" of Exhibit 4001 should be doubted. FED. R. EVID. 803(8)(B). Because the elements of Rule 803(8) are not met, the Court cannot admit Exhibit 4001 under the public records exception to the hearsay rule.

ii. The Emails Received by the FTC Are Not Admissible as Business Records.

Rule 803(6) provides a hearsay exception for records of a "regularly conducted activity of a business". FED. R. EVID. 803(6). First of all, the FTC is not a business; it is a government agency. If any exception under Rule 803 would apply, it should be the public records exception in subsection (8). 2 Kenneth S. Broun, et al., McCormick on

Evidence § 288 and fn. 37 (7th Ed. 2013) (prosecution must rely on public records exception, not regularly conducted activity exception, in seeking introduction of police reports).

Statements may not be admitted under the regularly conducted activity exception if they are prepared primarily for litigation. 2 Kenneth S. Broun, et al., McCormick on Evidence § 288 (7th Ed. 2013), *citing Palmer v. Hoffman*, 318 U.S. 109 (1943). Here, where the FTC has solicited the public's help in collecting these emails for preparing cases with its "law enforcement partners", every email in the FTC's spam database is intended for litigation, and should not qualify for this exception to the hearsay rule.

iii. The Emails Received by the FTC Cannot Be Authenticated.

Even if the Court were to find an exception to the hearsay rule, Exhibit 4001 must still be authenticated. The Government "must produce evidence sufficient to support a finding that the item is what the [Government] claims it is." FED. R. EVID. 901(a). Rule 901 provides for how public records may be authenticated, namely with "[e]vidence that: (A) a document was recorded or filed in a public office as authorized by law; or (B) a purported public record or statement is from the office where items of this kind are kept." FED. R. EVID. 901(b)(7).

While the FTC receives email and stores it, these documents are not "recorded or filed in a public office as authorized by law". FED. R. EVID. 901(b)(7). As the FTC's Privacy Impact Assessment states, the FTC created its spam database "[t]o support [its Bureau of Consumer Protection]'s investigations and consumer protection-related

activities…" However, no statute or regulation required or authorized this action, so it is not "authorized by law". Further, the plain meaning of "recorded or filed in a public office" means formal processes such as filing a document with a court clerk or county clerk-recorder's office.

e. The Vast Majority of the Emails in Exhibit 4001 Are Not Relevant.

It goes without saying that irrelevant evidence is not admissible. FED. R. EVID. 402. However, Mr. Livingston's review of Exhibit 4001 has revealed that the vast majority of its contents are irrelevant.

One example of plainly irrelevant email in the FTC dataset is an email from a tipster whose email address, because it ends in "yahoo.com.br", indicates he or she was from Brazil. (Halliburton Decl. ¶¶ 5–6 and Exs. 4–6; Declaration of Matthew Edman in Support of Defendant's Motions *in Limine* ("Edman Decl.") ¶¶ 22–23, 26.) (".br" is the top-level country domain for Brazil.[6]) This April 24, 2016 email (produced to the defense as "uce.2016042418.028286.eml") attaches two items of purported spam, both of which are in Portuguese, and both of which also originate from Brazilian domain names. The only apparent reason for these emails' inclusion is that they were transmitted from a server with an IP address the government believed was at some point in time connected to Mr. Livingston. That is the *only* connection to this case, and it is no connection at all because it is clear that this IP address corresponds to a server hosting company with numerous clients. (Edman Decl. ¶¶ 20, 22–23, 26.) Therefore these emails have absolutely no connection to Corporate Victim #1, no connection to

[6] https://www.iana.org/domains/root/db

Corporate Victim #2, and the dates fall two years after the conspiracy alleged in Count 1, and half a year after the conspiracy alleged in Count 2 and any other factual allegation in the Superseding Indictment. As for the IP address, it plainly belongs to a server hosting company with numerous clients. That shared server happens to have been used to send email to a user in Brazil, who then sent that email to the FTC. These emails are all plainly irrelevant.

Another tipster sent an email to the FTC on November 10, 2015 (produced to the defense as "uce.2015111012.020599.eml"). (Halliburton Decl. ¶¶ 5, 7 and Exs. 7–9; Edman Decl. ¶¶ 22, 24.) This email attached *thirty four* emails that were purportedly spam. Of these thirty four emails, one appears to have originated from another IP address the government believed was at some time connected to Mr. Livingston. (Halliburton Decl. Ex. 8.) Like the previous example, this IP address is also for a server hosting company with numerous clients. (Edman Decl. ¶¶ 20, 22, 24.) Moreover, this single email that matched the FTC's search criteria has nothing to do with Mr. Livingston. It is not at all connected with either Corporate Victim #1 or Corporate Victim #2. (Edman Decl. ¶ 27.) It also falls outside the time scope of any alleged conspiracy or other factual allegation in the Superseding Indictment. It is irrelevant, as are the thirty three other emails it was lumped in with by the tipster. Nevertheless, all thirty four irrelevant emails were included in Exhibit 4001.

There are highly prejudicial and inflammatory materials among these thirty four irrelevant emails. For example, one email comes from an email address with the domain

"botsnet.bw", which is registered to a telecommunications company in Botswana.[7] (Halliburton Decl. Ex. 9; Edman Decl. ¶ 24.) The email masquerades as an official notice from "U.S. Customs and Border Protection", and is clearly a scam. It has no connection whatsoever to any fact in this case: not to Mr. Livingston, not to Corporate Victim #1, not to Corporate Victim #2. (Edman Decl. ¶ 27.) As with the Brazilian emails, this scam email from Botswana was caught up in the FTC's vastly over-inclusive collection. For this scam email — and the countless others like it — to come into evidence would be highly prejudicial to Mr. Livingston. FED. R. EVID. 302.

These examples are only the tip of the iceberg. They strongly suggest that the methods the FTC used to prepare Exhibit 4001 for this case were vastly over-inclusive, and yielded more false positives than relevant evidence. (Edman Decl. ¶¶ 15–21, 26–27.) When evidence is not relevant, it is "not admissible". FED. R. EVID. 402.

f. Exhibit 4001 is Not Reliable.

The hearsay exceptions for regularly kept records and public records are "justified on grounds of trustworthiness and necessity…Reliability is furnished by the fact that regularly kept records typically have a high degree of accuracy." 2 Kenneth S. Broun, et al., McCormick on Evidence § 286 (7th Ed. 2013). But both at common law and under the Federal Rules of Evidence, these exceptions are unavailable when an opponent shows that the underlying evidence is not reliable. As discussed above, admitting unreliable hearsay evidence can be a Confrontation Clause violation. *Maryland v. Craig*, 497 U.S. 836, 845 (1990).

[7] https://www.iana.org/domains/root/db

Rule 803 guards against the admission of unreliable evidence under its hearsay exceptions. The regularly conducted activity exception may apply *only if* "the opponent does not show that the source of information or the method or circumstances of preparation indicate a lack of trustworthiness". FED. R. EVID. 803(6)(E). The public records exception shares nearly identical language; it may apply *only if* "the opponent does not show that the source of information or other circumstances indicate a lack of trustworthiness". FED. R. EVID. 803(8)(B).

i. The FTC Spam Database Accepts Email From Unknown Sources Without Vetting.

Exhibit 4001 is not reliable because it contains exclusively materials submitted by the general public, via the Internet and without verification or authentication, to the FTC. These facts recall the famous 1993 cartoon in *The New Yorker*:

Peter Steiner, *On the Internet, nobody knows you're a dog*, The New Yorker (Jul. 5, 1993).

Courts have struggled with similar facts in deciding whether to treat Wikipedia articles, which may be edited anonymously, as reliable evidence. *See*, *e.g.*, *Capcom Co.*

v. MKR Grp., Inc., No. C 08-0904 RS, 2008 WL 4661479, at *4 (N.D. Cal. Oct. 20, 2008) (denying request for judicial notice of Wikipedia articles), *citing Nordwall v. Sec'y of Health & Human Servs.*, No. 05-123V, 2008 WL 857661, at *7 n.6 (Fed. Cl. Feb. 19, 2008) ("Wikipedia may not be a reliable source of information.").

The same reliability concerns arise here, where the FTC apparently accepts, without any screening, all email it receives — even email containing dangerous "viruses and other malware". According to the FTC's Privacy Impact Assessment:

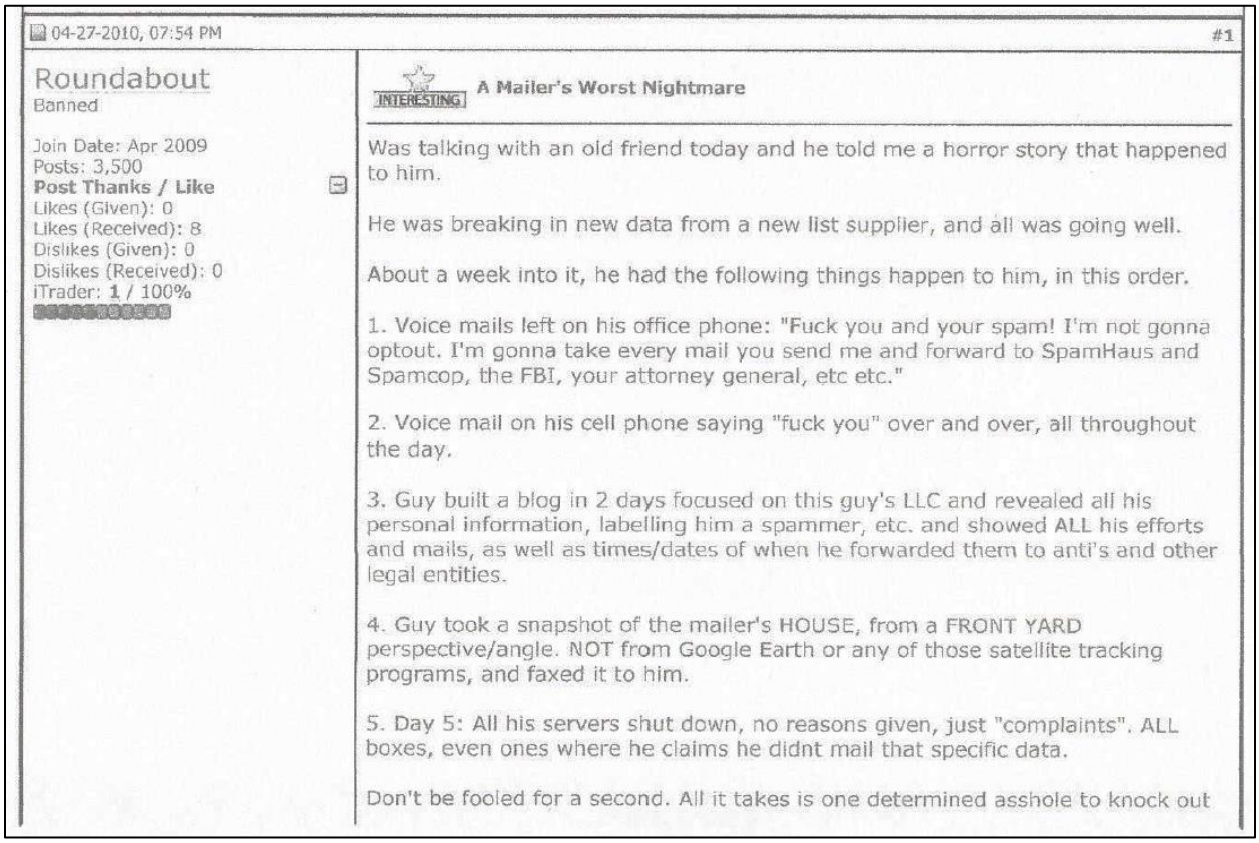
> Because email may contain viruses and other malware that can exploit security vulnerabilities and text messages may include links to harmful sites, the SpamDB receives and processes all emails and texts in an isolated cloud computing environment. The SpamDB permits authorized [Consumer Sentinel Network] users to view a static image of the actual email and texts to protect [Sentinel Network Services] and its users against any risks associated with spam email and text.

Federal Trade Commission, *Privacy Impact Assessment for Sentinel Network Services* (Jan. 2016) at p. 5, https://www.ftc.gov/system/files/attachments/privacy-impact-assessments/160114snspia.pdf [https://perma.cc/QE75-YVZP] (footnotes omitted).

ii. Anti-Spam "Activists" Are Known to Harass and Falsely Accuse Email Marketers.

Understandably, many members of the public dislike receiving unsolicited commercial email. However, some step well beyond the bounds of decency and even the law, and into harassment. The Government knows this because it collected examples of

this harassment when it searched Mr. Livingston's residence. For example, the Government seized printouts from an online message board where a poster talked about an email marketer being viciously harassed:



04-27-2010, 07:54 PM #1

Roundabout
Banned

Join Date: Apr 2009
Posts: 3,500
Post Thanks / Like
Likes (Given): 0
Likes (Received): 8
Dislikes (Given): 0
Dislikes (Received): 0
iTrader: 1 / 100%

INTERESTING **A Mailer's Worst Nightmare**

Was talking with an old friend today and he told me a horror story that happened to him.

He was breaking in new data from a new list supplier, and all was going well.

About a week into it, he had the following things happen to him, in this order.

1. Voice mails left on his office phone: "Fuck you and your spam! I'm not gonna optout. I'm gonna take every mail you send me and forward to SpamHaus and Spamcop, the FBI, your attorney general, etc etc."

2. Voice mail on his cell phone saying "fuck you" over and over, all throughout the day.

3. Guy built a blog in 2 days focused on this guy's LLC and revealed all his personal information, labelling him a spammer, etc. and showed ALL his efforts and mails, as well as times/dates of when he forwarded them to anti's and other legal entities.

4. Guy took a snapshot of the mailer's HOUSE, from a FRONT YARD perspective/angle. NOT from Google Earth or any of those satellite tracking programs, and faxed it to him.

5. Day 5: All his servers shut down, no reasons given, just "complaints". ALL boxes, even ones where he claims he didnt mail that specific data.

Don't be fooled for a second. All it takes is one determined asshole to knock out

Excerpt from paper documents seized by Government, labeled as evidence item 1B51 and produced to Mr. Livingston during discovery.

Another well-known method of harassing email marketers is the so-called "joe job": falsifying emails to make them appear to come from someone else. The Government's own technical expert has written about this phenomenon, and described it as "fairly common":

> The other reason it's a bad idea to fight abuse with abuse, is that you cannot be sure you know who your target is. So called joe jobs, in which

> someone sends out spam pretending to be from someone else, to make trouble for the someone else, are fairly common. Every spammer of course claims to be the victim of a joe job, not to be spamming himself, and sorting out the truth involves [sic] is not straightforward.

John Levine, *Abusive Anti-Anti-Spam Scheme a Dreadful Strategy*, CircleID (Jul. 26, 2005), http://www.circleid.com/posts/abusive_anti_anti_spam_scheme_a_dreadful_strategy [https://perma.cc/KDR9-6GV7].[8]

In a world where anti-spam "activists" are known to take such extreme — and unlawful — measures, and where the FTC does not verify the emails it receives, there is ample reason to doubt Exhibit 4001's reliability.

iii. At Least One Similar Trial Exhibit Has Been Tampered With.

Trial Exhibit 6001 is another clear example of the evidentiary problems the Government would like to sweep under the rug in this case. Exhibit 6001, which the Government describes incorrectly in its exhibit list as an "Email from Google to Corporate Victim #1", is actually *another anonymous tip*. It is an email from a Google mail account holder identified only as "Sam".

Unfortunately, it is evident that someone — perhaps, but not necessarily, "Sam" — tampered with this purported email. At the top of page 2, the email says "<link to malicious web site has been removed>":

[8] Mr. Livingston reserves his rights with respect to Mr. Levine, including but not limited to the *Daubert* motion and motion *in limine* regarding his expected testimony, *infra*.

abusenotification.txt

------=_NextPart_000_625C_01CE26C3.0255F8F0
Content-Type: text/plain;
charset="utf-8"
Content-Transfer-Encoding: 7bit

Let us help your sell your timeshare. Learn more:
<link to malicious web site has been removed>

Excerpt from Trial Exhibit 6001

Further, Exhibit 6001 is far from the best evidence: it appears to be an email that someone (we do not know who) copied and pasted into a separate file; then someone (we do not know who) printed that file onto paper. At some point (we do not know when) this evidence was materially altered (and we do not know by whom).

Mr. Livingston will move separately for the exclusion of Exhibit 6001. However, for the purposes of this motion, Exhibit 6001 illustrates the very serious problems with the FTC database in Exhibit 4001: unknown anonymous sources, potential *and actual* falsification, and multiple levels of hearsay — all without any ability for Mr. Livingston to cross-examine any witness with personal knowledge.

g. The Voluminous Nature and Imprimatur of the Federal Government on Exhibit 4001 Will Create a False and Highly Prejudicial Impression of Reliability.

Rule 403 exclusion is especially appropriate where evidence bears the imprimatur of the federal government and would lead the jury to give the evidence undue weight. *See e.g., Martin v. Cavalier Hotel Corp.*, 48 F.3d 1343, 1358 (4th Cir. 1995) (noting prejudicial effect that an official report might have on the jury); *In re Air Crash at Charlotte*, 982 F. Supp. 1060, 1066 (D.S.C. 1996) (excluding evidence of

federal government's admission, noting the jury might place undue weight on statements of an official government agency); *City of N.Y. v. Pullman, Inc.*, 662 F.2d 910, 915 (2d Cir. 1981) (affirming exclusion of government report where admission would likely protract an already prolonged trial into collateral issues regarding the accuracy of the report and methods used in its compilation); *John McShain, Inc. v. Cessna Aircraft Co.*, 563 F.2d 632, 636 (3rd Cir. 1977) (affirming exclusion of government reports where reception would have involved lengthy attempt to sift out admissible hearsay and inquiry into trustworthiness); *United States v. McElmurry*, 776 F.3d 1061, 1070 (9th Cir. 2015) (court must exercise its discretion in an informed manner and may not rely on the government's offer of proof).

Reference to Exhibit 4001, or the number of emails in it, undoubtedly creates a danger of unfair prejudice. As discussed above, the FTC's spam database is not an acceptable source of reliable information. The jury, however, would likely assume the opposite. If introduced, Exhibit 4001 would likely inflame the jury into finding liability under the incorrect assumption that the FTC database is reliable evidence, and that the volume of data, by itself, creates liability. The Exhibit will also confuse the issues and mislead the jury because Mr. Livingston will be forced to put on a mini-trial on collateral issues to dispute the validity of the database and emails.

A limiting instruction will not suffice. The imprimatur of the Federal Government on Exhibit 4001 alone will create a false and highly prejudicial impression of reliability and relevance. Moreover, introduction of the voluminous Exhibit (approximately 200,000 emails) will waste time and create needless presentation of cumulative

evidence, including rebuttal testimony to show lack of reliability and connection to Mr. Livingston.

Finally, the probative value, if any, is minimal and substantially outweighed by the danger of undue prejudice. Exhibit 4001 is not reliable evidence of Mr. Livingston sending specific emails to consumers, nor of the content of any alleged emails, nor of his role in any alleged conspiracy. The Court should exclude Exhibit 4001, and any reference to it or to the number of emails in it, under Rule 403.

h. Originals Not Produced

As the FTC's own public writings make clear, and as is clear from Exhibit 4001 itself, Exhibit 4001 does not contain "original writing[s]". FED. R. EVID. 1002. Instead, it contains emails purportedly forwarded to the FTC by unknown persons. For the reasons discussed above, it would be "unfair to admit" duplicates. Those reasons include, among others, that there is no way for Mr. Livingston to cross-examine these unknown persons; that similar evidence has been tampered with; and that the government's own expert has written that so-called "joe jobs" used to frame email marketers like Mr. Livingston are "relatively common". Under these circumstances, the Court should insist that originals be produced, and if the government does not do that, then its evidence must be excluded.

i. Conclusion

While the FTC's spam database may be useful as a source of high-level intelligence about spam activity, it is not an acceptable source of reliable evidence in a criminal trial. Using email forwarded unreliably and inconsistently by unknown persons

on the Internet as substantive evidence of an offense, without authenticating testimony from those who sent it and an opportunity to cross-examine them, violates the hearsay rule and Mr. Livingston's constitutional rights under the Confrontation Clause. The Court should exclude Exhibit 4001, and any mention of it at trial.

D. Government Exhibit 2030 should be excluded from evidence at trial, as it is not relevant, and any probative value is substantially outweighed.

Mr. Livingston seeks to exclude Government Exhibit 2030, which is an image found on his computer. This image is a photograph of a person with Down's Syndrome with the words "I wonder if…the feds will know I spammed hacked data." While this image and similar ones are popular and considered jokes among commercial emailers, it has no relevance in this trial. FED. R. EVID. 401, 402. Moreover, even if the Court determines that such an image is relevant (and the defense maintains that it is not), it is extremely prejudicial, and its prejudice substantially outweighs any relevance. FED. R. EVID. 403. It should be excluded from evidence.

E. Government Exhibit 6001 should be excluded from evidence at trial because the document is inaccurate, unreliable, unauthenticated, not the best evidence, hearsay, and more prejudicial than probative.

Trial Exhibit 6001 is an email from an unknown Google mail account holder to Corporate Victim #2.

a. Inaccurate Description

The Government's Exhibit list describes this document inaccurately as an "Email from Google to Corporate Victim #1". First, the email only purports to be from an

individual who was a Google *mail account holder*, but not from the company Google itself. Mr. Livingston requests that, if it does allow the admission of Exhibit 6001 despite Mr. Livingston's arguments below, the Court should require the Government to refer to it accurately and not imply that it is from Google. Describing the email inaccurately as coming from a famous and well-regarded company would unfairly prejudice Mr. Livingston because the jury would likely be impassioned to accord it more weight than it is due. FED. R. EVID. 403.

Second, the purported recipient of this email is the company the Superseding Indictment refers to as Corporate Victim #2, not Corporate Victim #1. While this is presumably a simple typographic error on the Exhibit list, an email to Corporate Victim #2 is not, of course, relevant to any determination about Corporate Victim #1. FED. R. EVID. 401.

b. Exhibit 6001 is Unreliable Because it Has Been Tampered With.

It is evident that someone — perhaps, but not necessarily, the unknown author identified only as "Sam" — tampered with this purported email. At the top of page 2 of Exhibit 6001, the email says "<link to malicious web site has been removed>":

abusenotification.txt

------=_NextPart_000_625C_01CE26C3.0255F8F0
Content-Type: text/plain;
charset="utf-8"
Content-Transfer-Encoding: 7bit

Let us help your sell your timeshare. Learn more:
<link to malicious web site has been removed>

Excerpt from Trial Exhibit 6001

Thus, the Government will not be able to authenticate or lay foundation for Exhibit 6001 under FED. R. EVID. 602 and 901 et seq. Exhibit 6001 is also far from the best evidence: it appears to be an email that someone (we do not know who) copied into a separate file; then someone (we do not know who) printed that file onto paper; then someone (we do not know who) scanned that paper. At some point (we do not know when) this evidence was materially altered (and we do not know by whom).

Under these circumstances, it is proper to invoke Rules 1002 and 1003, which require "an original writing", FED. R. EVID. 1002, and state that "A duplicate is admissible to the same extent as the original **unless a genuine question is raised about the original's authenticity or the circumstances make it unfair to admit the duplicate**." FED. R. EVID. 1003 (emphasis added). Here, it is plainly evident that Exhibit 6001 is not a duplicate of the original email that "Sam" purportedly received; "Sam" or someone else altered it. It is also apparent that the email was taken from its original form, copied, pasted into a file called "abusenotification.txt", printed, and scanned. We do not know how, when, or by whom any of these steps were performed, or whether any *other* changes were made to Exhibit 6001. Finally, there is no reason to apply Rule 1004, which — only under specific enumerated circumstances, none of which apply — allows "other evidence of the content of a writing". FED. R. EVID. 1004.

c. Hearsay

Exhibit 6001 is purportedly an email from an unknown Google mail account

holder to Corporate Victim #2. However, the email is inadmissible hearsay without any applicable exceptions, and Mr. Livingston's constitutional rights under the Confrontation Clause would be violated by its admission. *Crawford v. Washington*, 541 U.S. 36 (2004). The Court should therefore exclude Exhibit 6001 from evidence, and should preclude the Government from discussing it at trial.

A criminal defendant has the right to subject all "testimonial" statements to the "crucible of cross-examination." *Id.* at 61. If the defendant does not have the opportunity to cross-examine a witness, those testimonial statements are inadmissible — regardless of their admissibility under the rules of evidence or a determination that they are reliable. *Id.* ("[W]e do not think the Framers meant to leave the Sixth Amendment's protection to the vagaries of the rules of evidence, much less to amorphous notions of 'reliability.'").

While it is impossible to divine the intent of the unknown author of Exhibit 6001 absent his or her own testimony, the language of the email tends to indicate it was intended to be testimonial. By using the word "compromised", the unknown author of Exhibit 6001 implied strongly that criminal activity was behind the unsolicited email he or she had received from Corporate Victim #2's mail servers — *i.e.*, that the mail servers had been hacked. AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE (5th Ed. 2016), https://ahdictionary.com/word/search.html?q=compromised&submit.x=0&submit.y=0 ("2. To impair, as by disease or injury: an immune system that was compromised by a virus."); *see, e.g.*, *Three Men Arrested in Hacking and Spamming Scheme*, FBI,

https://www.fbi.gov/contact-us/field-offices/newark/news/press-releases/three-men-arrested-in-hacking-and-spamming-scheme (Dec. 15, 2015) (FBI press release regarding this case, alleging that "Livingston and Chmielarz allegedly hacked into the e-mail accounts of individuals and compromised and seized control of the mail servers of some of the corporate victims to further their spam campaigns"); *Member of Hacking Group Sentenced to Three Years in Prison for Intrusions into Corporate and Governmental Computer Systems*, FBI, https://www.fbi.gov/contact-us/field-offices/losangeles/news/press-releases/member-of-hacking-group-sentenced-to-three-years-in-prison-for-intrusions-into-corporate-and-Governmental-computer-systems (Apr. 16, 2015) (discussing "computer attacks that compromised computer systems"); Tom Mendelsohn, *Mark Zuckerberg's Twitter, Pinterest accounts compromised*, ARS TECHNICA, http://arstechnica.com/security/2016/06/mark-zuckerberg-twitter-pinterest-hacked/ (Jun. 6, 2016).

d. Unduly Prejudicial

The content of Exhibit 6001 is highly prejudicial to Mr. Livingston and has little, if any, probative value. In it, the declarant, known only as "Sam", says "Your mail server is compromised." As discussed above, in the computer context, the word "compromised" means that someone has been hacked — in this case, allegedly Corporate Victim #2. As discussed in detail in Mr. Livingston's Pretrial Motions, the Government's allegations regarding Corporate Victim #2 are that Mr. Livingston's former co-defendant, Tomasz Chmielarz, wrote a computer program that used publicly accessible forms on Corporate Victim #2's website, and used them in the same way a human user of the website would.

(Memorandum in Support of Mr. Livingston's Pretrial Motions (Dkt. 40-1) at 20–30; Superseding Indictment (Dkt. 35) at 8–10.) While this could have resulted in a volume of email that Corporate Victim #2 would not have subjectively wanted, it does not indicate that its "mail server is compromised" as the unknown "Sam" incorrectly stated in Exhibit 6001.

The statement in Exhibit 6001 is also purely speculative. There is no reason to believe the unknown "Sam" had any knowledge of how Corporate Victim #2's mail servers worked, nor whether they were, in fact, "compromised".

Because "Sam"'s statement is both incorrect and inconsistent with the Government's allegations in the Superseding Indictment, it would confuse the issues, mislead the jury, and unfairly prejudice the jury against Mr. Livingston. The Court should exclude Exhibit 6001 under Rule 403, which allows the Court to "exclude relevant evidence if its probative value is substantially outweighed by a danger of one or more of the following: unfair prejudice, confusing the issues, [or] misleading the jury…" FED. R. EVID. 403.

Exhibit 6001 has plainly been tampered with. Its chain of custody is hopelessly unclear. It contains multiple levels of testimonial hearsay, including from an unidentified anonymous declarant. It contains an incorrect statement that is inconsistent with the Government's allegations. Its admission would confuse the issues, mislead the jury, and work unfair prejudice against Mr. Livingston. The Court should thus exclude the Exhibit and any reference to it.

F. Government Exhibit 7011 should be excluded from evidence at trial because it is inadmissible hearsay, is more prejudicial than probative, is not authenticated, lacks foundation, and is not the best evidence.

Defendant Timothy Livingston moves *in limine* to exclude all evidence, testimony, and suggestion regarding the Government's Trial Exhibit 7011 (Amazon Abuse Report) as quadruple hearsay, irrelevant, unduly prejudicial, lacking foundation and authentication, and not the best evidence under Federal Rules of Evidence 401, 403, 602, 801–807, 901, and 1002.

a. Background

The Government's Exhibit 7011 contains a chain of emails purportedly relating to an abuse report received by Amazon and forwarded to Digital Treetop, which is an affiliate network. (Halliburton Decl. Ex. 1.) The first email in the chain, from Amazon to Digital Treetop, states that Amazon received a report that servers it was hosting on behalf of Digital Treetop had been reported as "linked to spam/unsolicited email".

First, as discussed in Mr. Livingston's pretrial motions and in particular by his marketing expert, reports like this are commonplace in the email marketing industry and do not, by themselves, indicate any illegal or improper activity. *See* prior Expert Declaration of Brian N. Benenhaley (Dkt. 40-7) ¶¶ 3(e), 7, 8(f).

Second, the Government will not be able to show Mr. Livingston sent the originating email. Instead, the email that triggered the abuse report was sent by someone else who was operating as a sub-affiliate under Mr. Livingston's primary affiliate account. An unknown email recipient then apparently reported that originating email as spam to Amazon. There is no information about who reported the email, nor

what the full report said, nor whether any of that undisclosed information was accurate. Amazon then transmitted some portion of this information to Travis Simonds, who then emailed West Harris. The Government apparently obtained Exhibit 7011 from a subpoena to Digital Treetop, an affiliate network where Mr. Simonds and Mr. Harris worked.

b. Exhibit 7011 should be excluded from evidence because it is Inadmissible Hearsay and does not fall within any of the Hearsay exceptions.

Under Rule 802 of the Federal Rules of Evidence, out-of-court statements are generally not admissible to prove the truth of the matter asserted. The Government undoubtedly seeks to prove the truth of the statements in Exhibit 7011 to show (incorrectly) that Mr. Livingston was emailing spam, not honoring opt-outs, and/or getting paid for spam emails. However, Exhibit 7011 contains four levels of inadmissible hearsay.

No hearsay exceptions apply to any layer of this multiple hearsay. "The fact that the Internet service providers may be able to retrieve information that its customers posted or email that its customers sent does not turn that material into a business record…" *United States v. Jackson*, 208 F.3d 633, 637–38 (7th Cir. 2000) (finding web postings were not subject to the business records exception and were unfairly prejudicial, irrelevant, not properly authenticated, and lacking trustworthiness); *see also Ira Green, Inc. v. Military Sales & Serv. Co.*, 775 F.3d 12, 18–21 (1st Cir. 2014) (finding 2012 emails describing conduct from 2011 not subject to the business records exception); *Farkalun v. Hanning*, 855 F. Supp. 2d 906, 921–22 (D. Minn. 2012)

(anonymous Internet postings were hearsay that were not authenticated). *Compare FTC v. World Travel Vacation Brokers, Inc.*, 861 F.2d 1020, 1023 n.4 (7th Cir. 1988) (noting magistrate judge refused to admit several Exhibits containing numerous unsworn consumer complaints), *with FTC v. Kitco of Nevada, Inc.*, 612 F. Supp. 1282, 1294 (D. Minn. 1985) (admitting sworn consumer *affidavits* under residual exception because they went to a material fact, were trustworthy, and were more probative than other evidence). Each statement contained in Exhibit 7011 stems from an unidentified person's initial report. There is no indication that this initial report was made contemporaneously with the claimed abuse, under oath, or to a Government agency. Further, Mr. Livingston could not subpoena or cross-examine the initial reporter of spam because that person is unknown. Accordingly, no layer of Exhibit 7011 falls under a hearsay exception, including the business record or residual exception.

Finally, admission of, or reference to, Exhibit 7011 would violate Mr. Livingston's rights under the Confrontation Clause. *Crawford v. Washington*, 541 U.S. 36 (2004).

c. Exhibit 7011 is More Prejudicial than Probative.

Under Rule 403, the Court may exclude evidence "if its probative value is substantially outweighed by a danger of…unfair prejudice, confusing the issues, misleading the jury, undue delay, wasting time, or needlessly presenting cumulative evidence." *See also Sprint/United Mgmt. Co. v. Mendelsohn*, 522 U.S. 379, 384 (2008) (courts have wide discretion in assessing admissibility).

Exhibit 7011 creates a danger of unfair prejudice because a jury will likely be impassioned to believe the unauthenticated hearsay statements are reliable evidence of

unlawful activity. The Exhibit will also confuse the issues and mislead the jury, and Mr. Livingston will be forced to put on a mini-trial on collateral issues to dispute the validity and content of the emails. This will no doubt waste time and create needless presentation of cumulative evidence. Further, the probative value, if any, is minimal, and is substantially outweighed by the danger of undue prejudice because the Exhibit is not connected to Mr. Livingston and is not reliable evidence.

d. Exhibit 7011 Lacks Authentication, Lacks Foundation, and is Not the Best Evidence.

Exhibit 7011 is further inadmissible because it lacks foundation, lacks authentication, and is not the best evidence under Rules 602, 901, and 1002. Information obtained from the Internet is "inherently untrustworthy." *St. Clair v. Johnny's Oyster & Shrimp, Inc.*, 76 F. Supp. 2d 773, 774–75 (S.D. Tex. 1999) (highlighting anyone "can put anything on the Internet"); *see also Victaulic Co. v. Tieman*, 499 F.3d 227, 236–37 (3rd Cir. 2007) (noting admission of company website raised authentication concerns); *United States v. Vayner*, 769 F.3d 125, 131–32 (2nd Cir. 2014) (finding webpage was improperly admitted because there was no evidence that defendant created the webpage or was responsible for its contents); *Wady v. Provident Life & Accident Ins. Co.*, 216 F. Supp. 2d 1060, 1064–65 (exhibits purportedly taken from defendant's website could not be authenticated because no proof of who authored documents or of accuracy of content); John Levine, *Abusive Anti-Anti-Spam Scheme a Dreadful Strategy*, CIRCLEID (Jul. 26, 2005), http://www.circleid.com/posts/abusive_anti_anti_spam_scheme_a_dreadful_strategy

[https://perma.cc/KDR9-6GV7] (noting "joe jobs", in which impostor sends out spam pretending to be from someone, else are "fairly common").

Thus, Exhibit 7011 contains multiple levels of hearsay, is unduly prejudicial, and lacks authentication and foundation. Mr. Livingston therefore moves *in limine* to exclude all evidence, testimony, and suggestion regarding Exhibit 7011.

G. Mr. Livingston objects to the chain of possession and the authenticity of the Government's Exhibits, and requests that the Government satisfy its burden with respect to this.

Rule 901 of the Federal Rules of Evidence requires that a proponent of evidence satisfy the requirement of authentication. The defense has noted that several pieces of evidence that the government has indicated it will introduce at trial have issues regarding their authenticity. Accordingly, the defense submits the Certification of Lorraine Gauli-Rufo, attached hereto, providing the bases for this assertion. Thus, Mr. Livingston requests that the items identified in the Certification not be admitted unless proper authentication and foundation is provided.

H. The Court Should Preclude the Government's Expert from Testifying on Topics for Which He is Not Qualified, and From Usurping the Court's Role in Explaining the Law.

Under Rules 403 and 702 et seq. of the Federal Rules of Evidence, and *Daubert v. Merrell Dow Pharm.*, 509 U.S. 579 (1993), Defendant moves *in limine* to limit Government expert John R. Levine's expert testimony to technical areas and government/corporate enforcement of spam policies, for which he is qualified. However, Mr. Livingston moves to preclude Mr. Levine from testifying about topics for which he is unqualified, and from usurping the Court's role in explaining the law.

Specifically, Mr. Livingston moves to preclude Mr. Levine from testifying about: (1) general industry practice in the performance marketing industry, including as it relates to affiliate marketing and bulk emails; (2) specific opinions about the performance marketing industry, including how "legitimate" and "traditional" mailers of bulk email make money; and (3) explanation of the law, including the CAN-SPAM Act. Mr. Levine lacks the qualifications to testify about these topics, and his anticipated opinions about them are based on speculation, assumed facts for which there is no admissible evidence, and purported facts that are demonstrably false or in contradiction to the Government's evidence. The anticipated testimony would also be unduly prejudicial, confusing, and not helpful to the jury.

On August 22, 2016, the Government served a letter pursuant to Federal Rule of Criminal Procedure 16(a)(1)(G), stating John R. Levine was expected to testify "regarding internet and electronic mail concepts, as well as spam and internet security." The letter, which attached Mr. Levine's curriculum vitae, provided various areas of expected testimony, which can be broken down into the following categories: (a) technical areas and government/corporate enforcement of spam policies; (b) industry/business practice in the performance marketing industry; and (c) explanation of spam laws.

The Government's letter and Mr. Levine's curriculum vitae demonstrate that Mr. Levine arguably has qualifications to testify about topic (a). However, Mr. Levine does not have any experience, education, publications, training, or other background to support his anticipated testimony on topics (b) and (c). (*See also* Declaration of Expert

Brian N. Benenhaley ("Benenhaley Decl.") in Support of Motion ¶¶ 3–5.)

Under Rule 702 and *Daubert*, 509 U.S. at 589–97:

> A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:
>
> (a) the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;
>
> (b) the testimony is based on sufficient facts or data;
>
> (c) the testimony is the product of reliable principles and methods; and
>
> (d) the expert has reliably applied the principles and methods to the facts of the case.

The primary analysis concerns qualification, reliability, and fit. *See Schneider ex rel. Estate of Schneider v. Fried*, 320 F.3d 396, 404–05 (3d Cir. 2003). "Qualification" refers to the requirement that the witness possess specialized expertise. *Id.* "Reliability" means the testimony must be based on methods and procedures of science, not subjective belief or unsupported speculation; the expert must have good grounds for his/her belief. *Id.* "Fit" means the testimony must be relevant and helpful to the facts. *Id.*

In determining whether expert opinion is reliable, courts may consider the following factors:

> (1) whether a method consists of a testable hypothesis; (2) whether the method has been subject to peer review; (3) the known or potential rate of

> error; (4) the existence and maintenance of standards controlling the technique's operation; (5) whether the method is generally accepted; (6) the relationship of the technique to methods which have been established to be reliable; (7) the qualifications of the expert witness testifying based on the methodology; and (8) the non-judicial uses to which the method has been put.

See Crowley v. Chait, 322 F. Supp. 2d 530, 536 (D.N.J. 2004) (*citing In re Paoli R.R. Yard PCB Litig.*, 35 F.3d 717, 742 (3d Cir. 1994)) (nothing requires admission of opinion evidence that is connected to existing data only by the say-so of the expert). *Compare Yarchak v. Trek Bicycle Corp.*, 208 F. Supp. 2d 470, 495–96 (D.N.J. 2002) (test is whether the opinion is based on valid reasoning or methodology, rather than whether the opinion has the best foundation or is demonstrably correct), *with Fedorczyk v. Caribbean Cruise Lines, Ltd.*, 82 F.3d 69, 75 (3d Cir. 1996) (judge may strike testimony if it is revealed on cross-examination that the opinion was based on inadequate foundation).

By means of a *Daubert* hearing, the district court acts as a gatekeeper, preventing testimony that does not meet the requirements of qualification, reliability, and fit from reaching the jury under Rule 104(a) of the Federal Rules of Evidence. *See Schneider*, 320 F.3d at 404–05; *Crowley*, 322 F. Supp. 2d at 537 (proponent bears the burden of establishing admissibility by a preponderance of the evidence); *In re TMI Litig.*, 199 F.3d 158, 159 (3d Cir. 2000) (*in limine* hearings are not required but often important); *McGlinchy v. Shell Chem. Co.*, 845 F.2d 802, 806–07 (9th Cir. 1988) (motions *in limine*

may be granted where opinion is based on assumptions that are unsupported by the evidence); *Nebraska Plastics, Inc. v. Holland Colors Am., Inc.*, 408 F.3d 410, 415–16 (8th Cir. 2005) (same); *Beech Aircraft Corp. v. United States*, 51 F.3d 834, 842 (9th Cir. 1995) (motions may challenge opinions that are not on proper subjects for expert opinion).

Because of the "powerful and potentially misleading effect of expert evidence," opinions may also be excluded under Rule 403. *United States v. Frazier*, 387 F.3d 1244, 1261–65 (11th Cir. 2004) (trial court's gatekeeping function requires more than taking the expert's word for it). Further, as a general matter, trial courts should exclude expert testimony that expresses a legal conclusion or usurps the role of the judge or jury. *See Hygh v. Jacobs*, 961 F.2d 359, 363 (2d Cir. 1992); Thomas Baker, *The Impropriety of Expert Witness Testimony on the Law*, 40 U. KAN. L. REV. 325, 338–39 (1992).

First, the government's summary of Mr. Levine's opinions shows that he is wholly unqualified to testify about industry/business practice in the performance marketing industry, including as it relates to affiliate marketing and bulk emails. Not only does Mr. Levine not have background, education, experience, or specialized expertise in this area, but one major factual representation is plainly incorrect — indeed, it is so wrong that it raises a red flag signifying extreme ignorance of the topic. Specifically, the government says that Mr. Levine will explain that affiliate marketers are paid based on how much email they send, as opposed to how many clicks, leads, or sales their emails generate. This statement, which the government presents as a fact within Mr. Levine's knowledge, is *unequivocally false*. It is the *opposite* of industry practice. (*See* Benenhaley Decl. ¶ 5,

Ex. A.)

The government's summary of Mr. Levine's opinions also conflicts with its own evidence, which shows that Mr. Livingston was *not* paid based on how much email he sent, but rather by *actions* resulting from those emails, like clicks, leads generated, and sales. For example, the Government's Trial Exhibit 7012 shows that one affiliate network was tracking statistics and paying Mr. Livingston on the basis of *leads — i.e.*, actions by consumers based on emails they received — not emails sent. Trial Exhibit 2020 also shows that Mr. Livingston was paid based on leads, not emails sent. (Halliburton Decl. Exs. 2–3; Benenhaley Decl. ¶ 6.)

Thus, Mr. Levine's expressed opinions are so manifestly wrong that he is unqualified to testify about how the performance marketing industry works, and how "legitimate" and "traditional" mailers of bulk email make money. Mr. Levine's testimony on these subjects would be inaccurate conjecture that would mislead and be unhelpful to the jury, not only because it is incorrect, but also because it conflicts with the Government's own documentary evidence.

It is also inappropriate for Mr. Levine to opine on the law. It is the Court's job to explain to the jury what the law is, not Mr. Levine's. However, the government's disclosure to the defense states that Mr. Levine's testimony will include, in relevant part:

> The Government expects Mr. Levine will also provide background regarding commercial e-mail distribution and spam. Mr. Levine will testify about the problems associated with spam and the enactment of the CAN-SPAM Act. He will further discuss CAN-SPAM and the implementation of the statute, including how CAN-SPAM covers false header information, deceptive subject lines, the identification of e-mails as advertisements, and use of real physical addresses. In addition, he will testify that CAN-SPAM requires opt-out options for recipients and that those that engage in

> legitimate bulk mailing (or hire others to do so) must maintain suppression lists.

In general, expert testimony is not permitted to explain the law. Levine is not qualified as a legal expert. Moreover, the testimony would be unduly prejudicial and interfere with the roles of the judge, jury, and counsel. The Government's opportunity to explain the law comes when it files proposed jury instructions — not when its witnesses are on the stand.

For these reasons, Defendant respectfully requests that the Court limit Mr. Levine's testimony to topics on which he is qualified, and preclude him from testifying about industry standards in the performance marketing industry, both generally and as to specific anticipated opinions, and from testifying about the law.

CONCLUSION

Based on the above, the Defendant respectfully requests that this Court exclude from evidence: A) any reference to "phishing" and/or the sign or picture "<><"; B) any reference to or introduction of any images or reference to Mr. Livingston's Ferrari or Cadillac Escalade vehicles at trial, and excluding Government Exhibits 2003, 2004 and 8001; C) Government Exhibit 4001 (FTC Search Data); D) excluding Government Exhibit 2030 (image of a man with Down's Syndrome found on Mr. Livingston's computer); E) Government Exhibit 6001 (notification of a Gmail user to Corporate Victim #2); F) Government Exhibit 7011 (an email thread produced by Digital Treetop), G) a ruling that the government must satisfy the requirements of Rule 901 prior to the admission of any evidence at trial; and H) testimony by the government's expert that is beyond his expertise, and that seeks to explain the law.

Respectfully submitted,

S/Lorraine Gauli-Rufo

LORRAINE S. GAULI-RUFO
LGR Law, LLC
130 Pompton Avenue
Verona, NJ 07044

KARL S. KRONENBERGER
ANSEL J. HALLIBURTON
KRONENBERGER ROSENFELD, LLP
150 Post St., Suite 520
San Francisco, CA 94105
Attorneys for Timothy Livingston